**国家信息安全漏洞共享平台(CNVD)漏洞通报**

**关于深圳市网心科技有限公司网心云设备存在未授权访问漏洞的情况通报**

国家互联网应急中心（CNCERT） 2023年3月20日

## 漏洞描述

fofa: app="网心云设备" && country="CN"



<http://183.215.133.34:9999/>

点击url直接登录后台



<http://110.82.88.86:9999/>

点击后登录



<http://223.84.29.150:9999/>

点击后登录



<http://110.82.88.9:9999/>



222.65.23.82:9999

223.75.170.161:9999

60.28.102.85:9999

61.188.231.28:9999

183.250.27.70:9999

183.214.205.40:9999

125.79.96.55:9999

42.85.151.57:8882

58.219.152.192:9999

183.234.153.41:9999

116.208.19.188:9*9*99

**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是由CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

**关于CNCERT**

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537